International Journal of Computer Science Engineering
and Information Technology Research (IJCSEITR)
ISSN(P): 2249-6831; ISSN(E): 2249-7943
Vol. 5, Issue 6, Dec 2015, 31-40

TRANS STELLAR
•Journal Publications •Research Consultancy

INTRUSION DETECTION SYSTEM AND PREVENTION SYSTEM IN CLOUD COMPUTING USING SNORT

SUNITA KUMAWAT[1], ANJALI KUMAWAT[2] & ANIL KUMAR SHARMA[3]

[1,2]*Research Scholar, Govt. Women Engineering College, Rajasthan, India*

[2]*Assistant Professor, Govt. Women Engineering College, Rajasthan, India*

ABSTRACT

As according to the current scenario, the security of the data is on threat and the protection from intruders is very important, organizations are paying a huge amount to secure their confidential data from intruders. But they are very sharp. Same as well the current systems are not capable enough to detect all the attacks which are occurring in the system. In order to fix this problem and to reduce the number of false alarms, intrusion detection method for the illegal access to the cloud server is proposed. Here in this article, we have proposed a hybrid model for intrusion detection system for cloud computing, which have enhanced quality of detecting the unknown attack via anomaly based detection and also have module which will try to reduce the number of false alarm generated by the system.

Keywords: Attacks, Intrusion, Cloud Computing, Snort Tool, System Security, IDS, Detection, Prevention

Received: Nov 13, 2015; **Accepted:** Nov 24, 2015; **Published:** Nov 28, 2015; **Paper Id.:** IJCSEITRDEC20155

Original Article

INTRODUCTION

Attacks on the nation's computer infrastructures are becoming an increasingly serious Problem. Even though the problem is ubiquitous, government agencies are particularly appealing targets and they tend to be more willing to reveal such events than commercial Organizations. This is demonstrated by the cases cited below. While statistics on the growth of attacks provide a more solid basis for justifying the need for intrusion detection (ID), case histories can often be more persuasive. Since many different mechanisms were opted by organizations in the form of intrusion detection and prevention systems to protect themselves from these kinds of attacks, there are many security breaches which go undetected. In order to understand the security risks and IDPS(intrusion detection and prevention system), we will first survey about the common security breaches and then after discuss what are different opportunities and challenges in this particular field.[1]

RELATED WORK

Intrusion detection system comprises of management unit and detection engine. The management unit is to manage the reporting part or manage how the output reports is generated if there is any intrusion is find and detection engine are agents that monitors host and network in real time environment. Intrusion detection system also has a database of attack signatures. These are the patters of different attacks which are attacked previously in the system the purpose of saving this database is that when a detection engine detects the malicious packet it first matches with the database of known signature of attacks and if match was successful it generate a message and pass to the management unit which further take appropriate actions regarding that malicious packet.

Signature Based Intrusion Detection System

The signature based intrusion detection system is used for detecting the known attacks in network. Signature can be a pattern of strings or characters which can be found in payloads of packets. This type of detection technology required a database which is a collection of previous attacks called as known attacks. As when packets come in network the system matches the signature of the packet with the signature of the known attacks stored in database if matches found then the system alerts the administrator about the attacks discovered. As this signature based intrusion detection system is based on the knowledge of the previous attacks so this method is also called Knowledge based intrusion detection system. The main advantage of this method is that the system administrator does not require any special kind of detection team to detect the attacks as only database of the previous attacks are required but this type of detection method cannot identified the new attacks or intrusions whose patterns does not match with the database also it is not easy to update the database on regular interval of time.

Anomaly Based Intrusion Detection

Attackers are very smart people. They often program such kind of vulnerabilities whose signature will not be available easily. They know how to beat the IDS by crafting new exploits, thus it became very much important to block or detect these attacks. [1][3] The mechanism known as Anomaly detection can be used for this purpose. Anomaly based detection technique uses profile matching mechanism i.e. normal behavior and abnormal behavior. Anything that is deviated from baseline of "NORMAL" will be treated as anomaly. Normal behavior can be feed into the system based on offline learning and research and the online learning while processing the network traffic. This technique consists of two phases Training phase and testing phase. In training phase the normal traffic profile are defined while as in testing phase the learned profiles are applied to new data. It's establish a profile of the subject's normal behavior, compare the observed behavior of the subject with its norm profile, and signal intrusions when the subject's observed behavior differs significantly from its normal profile.

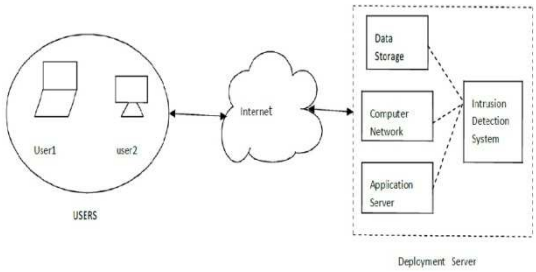

Figure 1: General View of the IDS System

CLOUD COMPUTING

In the recent years cloud computing technology is very popular for biggest organizations which deals with transfer of data from one location to another over the internet. Cloud computing have different perceptions from different users or peoples. To some it refers to the online service demand of software and storing the data in the cloud based system of the internet or a network and accessing the associated services and for some it refers the modernizations of the early system with the concept of time sharing of resources available in the network. Cloud computing model is reliable, convenient model which provides a shared set of resources to different users without any requirement of hardware and software suits.

As internet is a global public network and can be easily access from any part of the world. Through the use of

internet many organizations are reaching towards the end user potentially in the same time more and more people connected to the internet to excess the new business technology such as e-commerce which is most popular example of internet based services provided by different organizations besides these usefulness of internet it also produces some harms to the organizations. The user which connected to the network or the user which is a part of organization over the internet is harmless as long as it maintains the information securely over the network and the user which connected to the internet for stealing information and act as malicious user is called harmful user. This harmful user use various techniques to steal of acquire the important information about any organizations these techniques are Password cracking, Sniffing, encrypted text and many others. Sometimes these harmful users stick to the database and destroy all the information. Therefore it is important to develop security mechanism against these unwanted threats and apply some kind of security to entire level of the system from root level which detects the unwanted users these security model must woks with different/IP layer protocols to enhance the security from inside as well as outside users as many surveys declares that inside user is more harmful as they knows the system well and access the information more easily as compared to the outside hackers[18].

PROBLEM IDENTIFICATION AND DEFINITION

The purpose of this task is to create a new comprehensive hybrid model for improving Intrusion Detection and Prevention System in Cloud Computing.

The problem in [11] authors was not focused on providing experiments to prove the effectiveness of implementation of collaborative filtering algorithm constructed on the cloud model onto illegal access detection problem in the cloud computing environment.

In this paper [15] authors did not Implemented IDS architecture but used an apriori algorithm to detect frequent attacks. The future research will be including a feedback mechanism such that the frequent attacks detected by the IDS were updated to the signature database. This would ensure that it weren't remaining as an unknown intrusion in future.

SNORT SOFTWARE

After examining the different aspects of the problem and the past research in previous paragraph on Intrusion Detection and Prevention System in Cloud Computing problem, our research will focus on developing a **Hybrid Model for Intrusion Detection and Prevention System in Cloud Computing** with the following characteristics:

Traditional IDS such as Signature -based IDS will incapable of detecting unknown attacks. Anomaly - based IDS can detect those attacks. Applying the clustering algorithm separately for different connection attributes (duration, source bytes and destination bytes) improves the detection quality. The frequent attack detection module detects the frequent attacks, ensuring low false alarm rate and hence increasing reliability.

The cloud computing every user will unknown and detection of the authorized and unauthorized user will also very difficult, as cloud computing is virtual centralization. We can also say that detection of user's behaviour will also difficult. Due to this cloud computing provide services along with some terms and conditions. While user will request for the service Cloud Service Provider (CSP) provides authentication for the user. i.e. CSP provide username and password to the user for accessing services of the cloud. To track such type of users in CSP administrators have all the information of the users and it can avoid unauthorized actions in the cloud computing environment.

The proposed IDS we will try to detect various web services attacks such as wrapping attack, malware injection

attack as well as some system vulnerabilities. System vulnerabilities include session riding and hijacking or insecure cryptography etc.

Stateful Protocol Analysis

It depends on the protocol states that IDS could know and it is also called specification based detection Besides these commonly method of IDS there are various other modes/techniques of ids which are described as : Snort is a lightweight intrusion detection system it works on signature based methodology. Snort is open source intrusion detect ion which analyses the packet in the real time network and find different types of attacks snort has a very rich architecture which contains additional features of logging and alerting. Snort also support real time scanning of packets and provides the output in quick succession and works 24 hours a day. Snort examines the packets by monitoring it and captures the useful information and stored them for further processing. After capturing the useful information of packets it allow different modes of detection on these data and pass the data for matching. Thus snort is working like a vacuum container which puts all the information in one pool and the match with the list of items. This feature of detection provides by snort is very much useful in detection in large and complex network but it is lightweight intrusion detection system as it works on small requirements does not demand a specialized server and runs on a different types of operating systems.

Snort has mainly three aspects

Packet Sniffer of Packet Capture Module This mode is used for capturing the packets from the network and placed them in container for further processing.

Packet Log Mode log data in text file and log packets to the disk.

Rules Rules are the certain set of commands which is written in any language by the user. Rules can be easily read and modify. Snort checks packets against these series of rules in detection part.

Snort Component

Packet Data in the network which is to be detected for malicious attacks or activities.

Packet container Captures all the networks in the traffic. It is device used to collect the data networks either in form of hardware and software. In case of scenario of internet this packet container consists of IP traffic which includes many different higher layer protocols and packet container analyzes the network protocols to represent the packet in the human readable. Packet container performs activities like:

Network monitoring and troubleshooting

Performance measures and analysis of benchmarking

Converting the networks data into simple readable codes

Preprocessor This part is used to collect all the packets from the packet container and perform some actions on the packets to determine the behavior of the packets and also determine how the packets perform in the detection mode. The pre-processor use many Plug-INS these are the small programs that are written to validate the API of Snort. In preprocessor as soon as raw packets arrived it checks the packet against plug –in for determining the behavior of the packets and to finds out how these packets will behave in the detection phase snort uses many kind of PLUG- IN and their protocols and other layered protocols most commonly used Plug in are RPC, HTTP, and Port Scanner and associates

protocols are IP fragmentation protocols, flow control and HTTP pre-processor handler. These Plug-in can be activate and deactivate as they are needed in the pre-processor level. This feature of plug provide additional feature to pre-processor to completely analyze the packet before passes to the next step of detection.

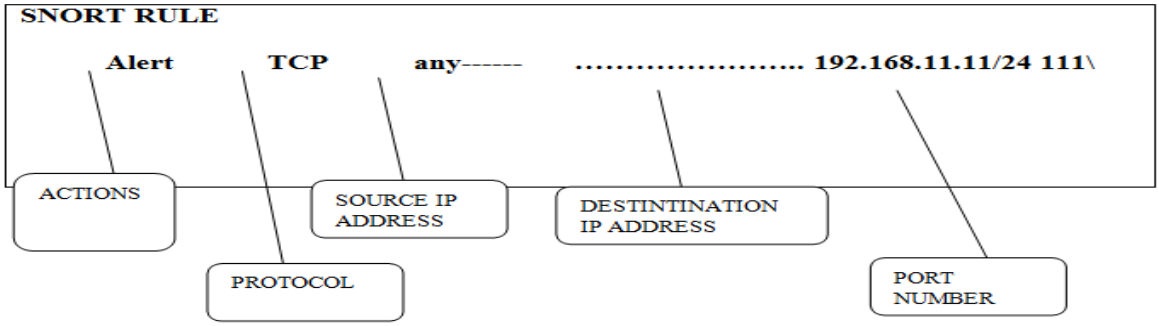

Figure 2: Snort Rule Model

Actions - Alert, log, pass, drop, reject

Protocol Type- TCP, UDP, IP, ICMP

IP Addresses- source IP address of machine

Port Number – Defines the range of port of IP address

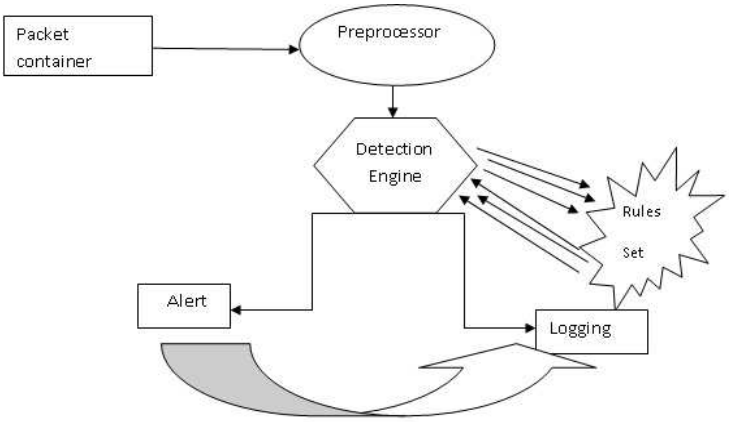

Figure 3: Architecture of Snort

Rule options are the main component of the intrusion detection Engine. Rule options are separated from each other using semicolon; and keywords are separated from their arguments with colon.

Detection module- detection module is the signature based IDS detection system. This phase uses various rules for detection if the rules match the data in the packet they are passed to the alert processor.

Logging and alerting –This part is called the output part and used to store the attacks which is detected. If data of packets is match with data in rules file in detection engine an alert is generated and can be send to log file through UNIX codes or through network connections. Alerts can also be recorded in MYSQL. We can also use other tools to display the alert file in web interface. By default logs are stored in text files.

Rule Sets – These are the grouped of different rules. Rules are divided into two parts:

Rule Header – Rule header is the information about actions to performed (alerts and log), type of network packets (TCP, UDP, ICMP). Source and destination IP address and ports

Rule Option – This contains the content in the packet that should match with the rules.

IDS IMPLEMENTATION AND RESULT ANALYSIS

Proposed Intrusion Detection System Architecture Model

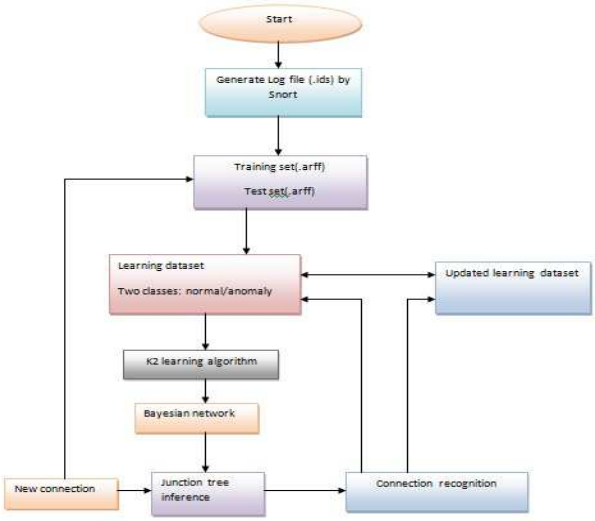

Figure 4: Proposed Architecture of IDS MODEL

Proposed Intrusion Detection System Algorithm

Step 1: Install snort, weka and netbeans

Step 2: Create snort.config file holding the ip address of the cloud server/system

Step 3: Access the internet and create log files using snort

Step 4: By these log files, generate two datasets (.arff files) for testing and training using weka

Step 5: Step 6: Apply K2 learning algorithm on the training and test datasets

Step 6: Now, using Bayesian algorithm create a junction tree

Step 7: Check new connections

If new connection < threshold

Then update the learning datasets

Else no change

Step 8: Exit

Implementation of Results and Analysis

Users Analysis in System

In this table, the legitimate and illegitimate users are shown. Also the users are divided into host and guest. The intruders are detected as anomaly.

Table 1: Users Find in System

Attributes	Normal	Anomaly
logged_in	19487	56636
is_host_login	67643	58631
is_guest_login	66471	58317
land	67337	58613

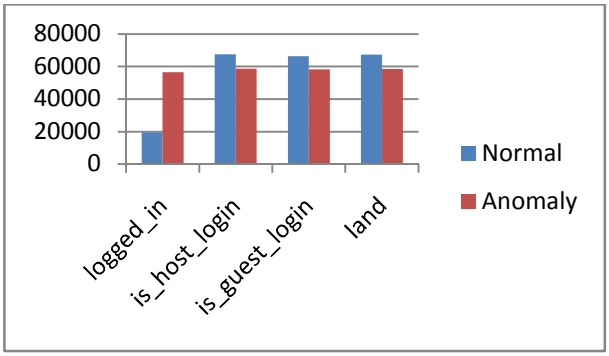

Figure 5: Users Analysis in IDS

Protocol Finds in Normal and Anomaly Intrusion Detection

This table shows all the protocols found in the system and differentiates them as normal and anomaly.

Table 2: Protocols in IDS

Protocols	Normal	Anomaly
tcp	53601	49090
udp	12435	2560
icmp	1310	6983

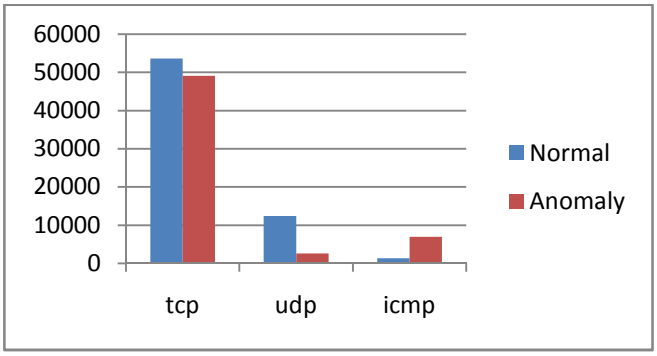

Figure 6: Protocols Analysis in IDS

Services Analysis in Normal and Anomaly Intrusion Detection

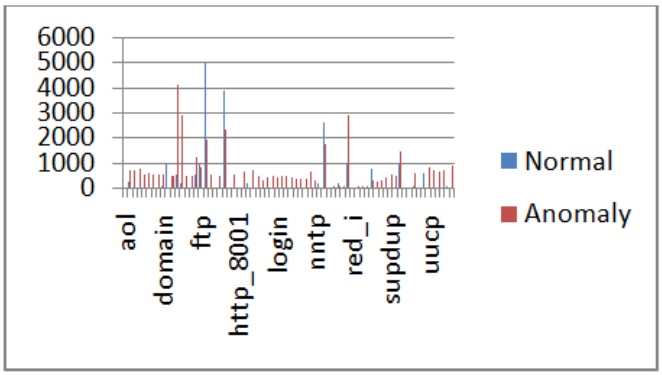

Figure 7: Service Analysis in IDS

Flag Implementation and Analysis in IDS

This tables represents flag analysis of the cloud infrastructure. The types of flag and the number of intrusions/anomalies are shown in the table.

Table 3: Flag identification

Flag	Normal	Anomaly
OTH	12	36
REJ	2694	8541
RSTO	220	1344
RSTOS0	1	104
RSTR	147	2276
S0	355	34498
S1	362	5
S2	120	9
S3	46	5
SF	63394	11553
SH	3	270

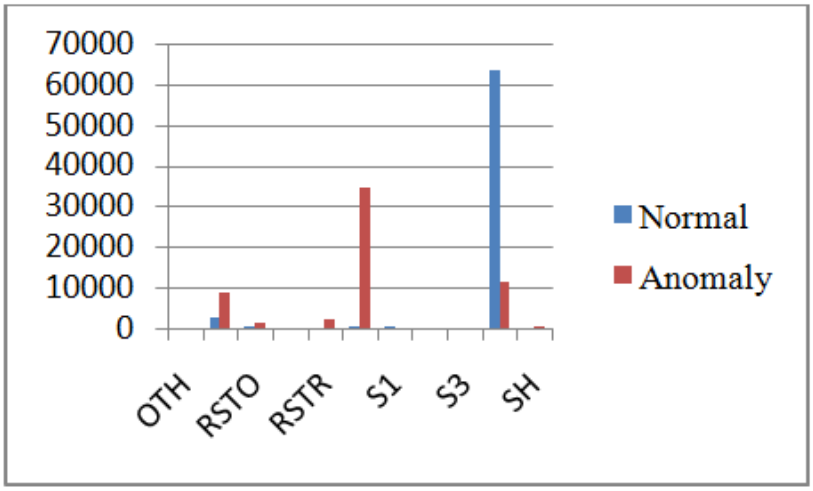

Figure 8: Flag Analysis in IDS

CONCLUSIONS

Cloud computing has generated significant interest in both academia and industry, but it's still an evolving paradigm. The proposed solution can significantly reduce the risk of the cloud system from being exploited and abused by internal and external attackers. The SA (Scenario Attack) algorithm achieves both control of requests and mugger identification. The need for reliable defenses is a crucial element in cloud architecture. Traditional IDS such as Signature - based IDS were incapable of detecting future unknown attacks. Anomaly - based IDS can detect those attacks. Applying the clustering algorithm separately for different connection attributes (duration, source bytes and destination bytes) improves the detection quality. The frequent attack detection module detects the frequent attacks, ensuring low false alarm rate and hence increasing reliability. Our Proposed System also allows to set new signatures without disturbing previous signatures. We will try to set new set of signatures for new attacks or unknown attacks and forward it to the Behavior-based IDS , so that in future same type of attack is knows by Behavior-based IDS and it will detected by Behavior-based IDS only. With the help of IDS definitely we will reduce false alarm rates. At the same time we can say that it will also detect unknown attacks also. In the proposed system we will use normal behavior of the system and signatures of various attacks to detect intrusions which is a hybrid IDS.

REFERENCES

1. *SAKURAI, Kouichi, and Tai-hoon Kim, "A Trend in IDS researches", (Journal of Security Engineering) Vol. 5, No. 4 (2008): http://www.sersc.Org/journals/JSE/vol5no42008/3.pdf.*
2. *Julia Allen, Alan Christie, William Fithen, John McHugh, Jed Pickel, Ed Stoner ,"State of the Practice of Intrusion Detection Technologies", TECHNICAL REPORT CMU/SEI-99-TR-028 ESC-99-028 ,2000.*
3. *Thomas M. Chen, Jorge Blasco, Jafar Alzubi, Omar Alzubi, "Intrusion Detection", IET Engineering & Technology Reference, Thomas M. Chen et al., pp. 1–9, doi: 10.1049/etr.2014.0007, ISSN 2056-4007, 2014.*
4. *Farah Jemili, Dr. Montaceur Zaghdoud, Pr. Mohamed Ben Ahmed, "A Framework for an Adaptive Intrusion Detection System using Bayesian Network", RIADI Laboratory, ENSI, Manouba University Manouba 2010, Tunisia,1-4244-1330-3/07/ 2007 IEEE.*
5. *Mostaque Md. Morshedur Hassan, "Current Studies On Intrusion Detection System, Genetic Algorithm And Fuzzy Logic", International Journal of Distributed and Parallel Systems (IJDPS) Vol.4, No.2, March 2013.*
6. *Bilal Maqbool Beigh, "One-Stop: A Novel Hybrid Model for Intrusion Detection System", International Conference on "Computing for Sustainable Global Development", INDIACom-2014, ISSN 0973-7529; ISBN 978-93-80544-11-3, 5th– 7th March, 2014.*
7. *Uzair Bashir and Manzoor Chachoo, "Intrusion Detection and Prevention System: Challenges & Opportunities", International Conference on "Computing for Sustainable Global Development", ISSN 0973-7529; ISBN 978-93-80544-11-3, 5th – 7th March, New Delhi (INDIA), INDIACom-2014.*
8. *Brojo Kishore Mishra, Minakshi Sahu, Satya Naryan Das, "Intrusion Detection Systems for High Performance Computing Environment", ICHPCA-2014, ISBN: 978-1-4799-5957-0, Bhubaneswar, India, December 22-24, 2014.*
9. *M. A. Aydin et al., "A hybrid intrusion detection system design for computer network security", Computer and Electrical Engineering, vol. 35, pp. 517–526, 2009.*
10. *Eugene C. Ezin, Herv´e Akakpo Djihountry ,"Java-Based Intrusion Detection System in a Wired Network", International*

Journal of Computer Science and Information Security, Vol. 9, No. 11, pp 33-40 ,November 2011.

11. *Rasim Alguliev, Fargana Abdullaeva, "Illegal Access Detection in the Cloud Computing Environment", Journal of Information Security, Vol 5, pp 65-71. http://dx.doi.org/10.4236/jis.2014.52007.*
12. *S.V. Narwane, S. L. Vaikol, "Intrusion Detection System in Cloud Computing Environment", International Conference on Advances in Communication and Computing Technologies (ICACACT) 2012.*
13. *Giriraj Vyas, Sanjay Meena, Pramendra Kumar, "Intrusion Detection Systems: A Modern Investigation", International Journal of Engineering, Management & Sciences (IJEMS), ISSN: 2348 –3733, Volume-1, Issue-11, November 2014.*
14. *Hemangini J. Patel, Riddhi Patel, "A Survey on Intrusion Detection System in Cloud", International Journal of Engineering and Technical Research (IJETR), ISSN: 2321-0869, Volume-2, Issue-5, May 2014.*
15. *P. Padmakumari, K. Surendra, M. Sowmya and M. Sravya, "Effective Intrusion Detection System For Cloud Architecture", ARPN Journal of Engineering and Applied Sciences, VOL. 9, NO. 11, NOVEMBER 2014, pp 2135-39, ISSN 1819-6608,*
16. *Hifaa Bait Baraka, Huaglory Tianfield, "Intrusion Detection System for Cloud Environment", Proc. SIN '14, September 09 - 11 2014, Glasgow, Scotland Uk,ACM 978-1-4503-3033-6/14/09.*
17. *Modi, D. Patel, A. Patel and R. Muttukrishnan, "Bayesian Classifier and Snort based network intrusion detection system in cloud computing", Computing Communication Networking Technologies (ICCCNT), Coimbatore, India, pp. 1-7, 26-28July,2012.*
18. *Asifahmed Algur, Ganesh Pai, "Nice: Network Intrusion Detection And Countermeasure Selection In Virtual Network Systems", Journal Of International Academic Research For Multidisciplinary, Impact Factor 1.393, Issn: 2320-5083, Volume 2, Issue 4, May 2014.*